SOC 2 in Plain English

A Readiness Field Guide for Small Teams — Volume 1: Getting Audit-Ready

Sylvan Press

Sylvan Press

Field-tested, plain-English references for the people who do the work and stand behind their call.

SOC 2 in Plain English

A Readiness Field Guide for Small Teams, Volume 1: Getting Audit-Ready

Published by Sylvan Press, the security imprint of Sylvan Assurance, LLC, Vermont, USA.

ISBN (paperback): 9798951893604
ISBN (hardcover): 9798951893611
ISBN (ebook): 9798951893628

First edition, 2026.

Disclaimer. This book provides general guidance and recommended security and compliance practices, not legal, financial, or professional advice, and it does not create any advisory or consulting relationship between the author, the publisher, and the reader. Every recommendation is optional: a widely accepted way to reduce a common risk, and the reader decides which to adopt, adapt, or decline. Following this guidance reduces exposure to common risks but does not guarantee any particular outcome and does not prevent any particular breach, incident, or loss. Where this book refers to laws, regulations, standards, or commercial products, it does so for general awareness only; confirm specific obligations with qualified counsel, and note that product references are illustrative and do not constitute endorsement.

Sylvan Press, sylvanassurance.com

Contents

Preface

Why this book exists

A customer asks a small software company for its SOC 2 report, and the company does not have one, or, more often, is not entirely sure what one is. That moment is where almost everyone meets SOC 2, and it is rarely a calm one. A deal that was nearly closed suddenly hangs on a document nobody can produce, attached to money the company was counting on. So the founder does the natural thing: opens a search engine, types in the question, and lands in a wall of vendor blogs, each one confident that the answer is to buy its product.

This book exists because of what usually happens next. Before anyone has explained what SOC 2 actually is, the quotes start to arrive, a compliance tool here, a readiness consultant there, the audit itself, and they add up fast. It is not unusual for the first round of numbers to total something close to twenty thousand dollars, aimed at a team that does not yet know which type of report it needs, which criteria belong in scope, or whether it needs half of what it is being sold. The stress of a deadline meets the confidence of a sales pitch, and expensive, hasty decisions follow.

This book is the plain-English explanation that should come first. It is the thing that founder should have had in hand before the quotes arrived: a calm walk through what SOC 2 is, what it is not, what it genuinely takes, and how a small team can get itself ready without panicking or overspending. The goal is modest and practical: to replace

the jolt with a plan, so that by the time you talk to a tool vendor, an auditor, or a consultant, you are buying on purpose rather than out of fear.

The book is for the person reading that procurement email for the first time, two browser tabs deep, wondering how something they had barely heard of last week became the thing standing between them and their biggest deal. There is a real answer underneath the marketing, and it is more reassuring than the panic suggests. This book is that answer.

What this book is and is not

This book explains SOC 2 (and its close cousin, ISO 27001) in plain English, and walks a small team through getting itself audit-ready. It is written to be understood by people who are not security experts, and to leave you with a clear picture of what the audit will expect and an honest plan for closing the gap. It is not a substitute for an auditor: your auditor performs its own examination and forms its own opinion based on your specific facts, and nothing in these pages changes that. It is not legal advice; where regulations or standards come up, they appear for general orientation, and the obligations that apply to your organisation are for qualified counsel to confirm. And it is deliberately not vendor-specific; it explains how compliance tools and auditors work, and when each earns its fee, without steering you toward any one of them. Where a topic has its own companion in this series (answering security questionnaires, or handling a security incident) the book points you there rather than trying to do that work in passing.

What this book assumes of the reader

This book is written for founders, operators, and first security or compliance hires at software companies of roughly five to two hundred people: the people who get handed "the SOC 2 thing," usually with no playbook and no prior experience. You are smart and busy, and you do not have time for a textbook; you have a deal to save, or a programme to stand up, and you want to understand this well enough to make good decisions quickly. That is the reader it is built for.

No security background is assumed. You do not need to know what a Trust Services Criterion is, or how an attestation differs from a certification: the book builds all of that from the ground up, expanding each term the first time it appears. What it does assume is that you have some familiarity with running software: that you have shipped a product, managed access for a team, dealt with a cloud provider, and understand at a working level how your own systems hang together. If you can describe what your company does and where its data lives, you have enough to start. The rest, this book supplies.

A note on defensibility

This book frames its recommendations as widely accepted practices rather than absolute requirements. Where the book recommends an action, the recommendation reflects what reduces risk in real operations, not a claim that any single action guarantees a particular outcome. The terms "is intended to," "reduces the likelihood of," and "is a recommended way to" carry that meaning consistently throughout. Where the book references regulations or standards, it does so for general awareness; specific obligations are for qualified legal counsel to confirm in your context.

Acknowledgements

This book is built from the published record of small teams meeting SOC 2 for the first time: auditors' own guidance, practitioner write-ups, and the questions asked and answered in public wherever founders compare notes. A plain explanation, offered at the right moment, has turned many an expensive decision into a sensible one; with thanks to the practitioners who wrote those explanations down, and whose hard-won judgement runs quietly through these pages.

How to Use This Book

You can read this book straight through, and the order is built to make sense that way: each part rests on the one before, and the vocabulary that feels like fog in the first chapter has cleared by the end of Part I. But most readers come to a book like this with a particular reason, and a particular amount of time, so here are a few reading paths depending on where you are standing right now.

If a deal is blocked on a SOC 2 today, and you need to understand your options and your money before you reply to anyone, start with Chapter 7, *The Honest Cost and Timeline*, and Chapter 9, *The Readiness Gap Assessment*. Chapter 7 puts the real numbers on the table and shows the cheaper paths the vendor guides will not mention; Chapter 9 shows you how to size the gap between where you stand and where the audit expects you to be. Together they turn the panic into a budget and a plan in an afternoon. Then circle back to Part I when you have a moment, so the plan rests on understanding rather than guesswork.

If you are exploring (SOC 2 has come up, perhaps from an investor or a forward-looking customer, and you want to understand it before it becomes urgent), read in order, front to back. You have the luxury most readers do not, which is time, and the book is at its best when you let it build the picture piece by piece before you spend any money.

If you are the first security or compliance hire, brought in to stand up a programme, read Parts I through III closely to get the lay of the land, then treat Part IV, *The Controls, in Plain English*, as your work-

ing reference, returning to whichever control area you are building or fixing. The book's framework, the Readiness Ladder, introduced in Chapter 9, gives you a simple way to track how far along the company is and to explain that progress to the people you report to.

If you do this for several companies at once, a fractional Chief Information Security Officer (CISO), a managed-service provider, or a consultant, the book is laid out so you can hand clients the relevant chapters and run a consistent process across all of them. The recurring fractional CISO in these pages, Priya Nair, stands in for exactly your situation, and her asides flag the places where doing this efficiently across many small clients differs from doing it once.

The four appendices are reference tools, and they differ from the chapters in kind. The chapters explain; the appendices are things you use. **Appendix A: The SOC 2 Readiness Checklist** is the gap-assessment instrument you run in Chapter 9, ordered by the Common Criteria, with status columns to fill in. **Appendix B: The SOC 2 to ISO 27001 Crosswalk** maps the criteria to the matching ISO 27001:2022 controls, so you can see how one set of work answers both frameworks. **Appendix C: A Plain-English Glossary** defines every term the book uses in a sentence or two. **Appendix D: The Document and Evidence Index** lists the policies and evidence items an audit expects, grouped by control area, each with a short "what good looks like" note. Keep them to hand; the chapters tell you when to reach for each.

The shape of this volume

This volume is laid out in five parts, each building on the one before.

Part I: What SOC 2 Actually Is (Chapters 1 through 5). The plain-English foundations. Why a customer asked for your SOC 2 in the first place; the whole model in one chapter, the AICPA attestation, the accounting firm that performs it, and the vocabulary of criteria, controls, and evidence; the difference between a Type I and a Type II report and which you need first; the five Trust Services Criteria and how to scope to the ones buyers actually ask for; and how SOC 2 relates to ISO 27001 and to the security questionnaires that arrive alongside it. By the end of Part I, the words stop being a fog.

Part II: Scoping and Planning (Chapters 6 through 8). The deci-

sions that set your cost and effort. What "your system" means and where to draw its boundary; an honest, numbers-on-the-table look at what SOC 2 costs and how long it takes, including the cheaper paths; and how to choose between doing it yourself, buying a compliance platform, or hiring an auditor, a consultant, or a managed-service provider.

Part III: The Readiness Assessment (Chapters 9 and 10). The heart of the book. How to look honestly at where you stand today, find the gaps between that and what an audit expects, and turn those gaps into a plan you can work through, using the book's own framework, the Readiness Ladder, and the checklist in Appendix A. And why a binder of policies is not the same as evidence, and how to collect evidence as you go rather than the night before fieldwork.

Part IV: The Controls, in Plain English (Chapters 11 through 15). A walk through the security practices an auditor will actually sample, each in everyday language: access control and identity; change management and the development lifecycle; risk assessment and vendor management; monitoring, logging, and incident response; and availability, backups, and continuity. Every chapter ends by naming the evidence the auditor will expect to see.

Part V: Crossing the Line (Chapter 16). The hand-off. Closing the last gaps, starting the clock on a Type II observation period, living the controls day to day, running the kickoff with your auditor, and what can still go wrong and how to recover, plus a look ahead to what comes after.

The other volumes

This is the first of a three-volume set, and each volume stands on its own, you do not need all three to get full value from one, but the set is designed to carry a company the whole way, from the first confused email to a mature, repeatable programme. Knowing what each volume is for helps you read the right book for where you are.

Volume 1: Getting Audit-Ready is this book. Its one job is to take you from "a customer asked for our SOC 2" to "we understand what we need, and we are ready for the audit to begin." It stops, deliberately, at the edge of the audit itself, because getting ready is the part where small teams most often overspend, stall, or go wrong.

Volume 2: The Audit and Operations picks up where this one leaves off. It covers the auditor relationship and the fieldwork itself, the day-to-day work of running controls and gathering evidence continuously, what happens at renewal each year, and a deeper treatment of the ISO 27001 information security management system. If Volume 1 gets you to the start line, Volume 2 is about running the race and keeping on running it.

Volume 3: The SOC 2 Operator's Workbook is the hands-on companion: the templates, the policies, the evidence trackers, and the gap-assessment worksheets, the fill-in-the-blanks versions of the tools this book describes, paired with a software toolkit for teams who want the worksheets in a more interactive form. Where Volumes 1 and 2 explain, Volume 3 hands you the instruments.

Each volume stands alone. Each is modestly priced in ebook.

About This Book

Structure

The book is organised in five parts and four appendices; "The shape of this volume," a few pages back, walks each in detail.

Defensibility statement

The book frames its recommendations as practices that reduce risk and improve audit readiness in real operations, not as actions that guarantee a particular audit outcome. A SOC 2 report is the product of an independent examination, and the service auditor forms its own opinion based on your specific facts; whether your controls satisfy the Trust Services Criteria is determined by that examination, not by adherence to any one book's recommendations, including this one. Where the book describes a control or a practice as something an auditor will look for, the description reflects what holds up in real readiness work, not a promise that it will satisfy your auditor in your circumstances.

This is not legal advice

Nothing in this book is legal advice, and nothing in it should be treated as a substitute for legal advice. The book is written to help operators understand SOC 2 and get their organisations ready; the specific obligations that apply to your company, under your contracts, in your jurisdiction, with respect to the data you handle, are for qualified counsel to confirm. Where the book describes a regulation, a standard, a

contractual term, or a deadline, the description is intended for general orientation and may not reflect the current state of the law or the framework at the moment you read it. Confirm specifics with counsel before acting on them.

Framework as of date

The content of this book reflects the state of the SOC 2 framework as of mid-2026. SOC 2 is an attestation governed by standards published by the American Institute of Certified Public Accountants (AICPA), and only a licensed Certified Public Accountant (CPA) firm can perform the examination and issue the report; the auditor forms its own opinion, and no book determines the outcome of that examination. References to ISO 27001 reflect the ISO 27001:2022 revision of the standard. Cost figures, timelines, and other ranges in the book are illustrative, they are meant to give you a sense of scale, not a quotation, and the market for tools, auditors, and consultants moves. Treat the dates, the figures, and the specifics here as a starting point for your own current research, and confirm anything that matters with your auditor and your counsel.

Conventions used in this book

Acronyms are spelled out the first time they appear, SOC 2 (System and Organization Controls), TSC (Trust Services Criteria), AICPA, CPA, MFA (multi-factor authentication), DPA (data processing agreement), ISMS (information security management system), and the rest, so you are never expected to carry a term you have not been given. The recurring companies in these pages, Atlas Freight, Harbor Books, Marlowe Health, and Vantage Cloud, along with the fractional CISO Priya Nair, are fictional; they are built from the patterns small software companies actually fall into, and they are there so you can find the one that looks most like you. Each chapter ends with a short *Recap* of its main points and a one-line *Next* pointer to the chapter that follows. The spelling is British English, except in proper nouns, official titles, and quoted material, which keep their original spelling.

The first chapter begins on the next page.

1 Why a Customer Asked for Your SOC 2

It is a Thursday afternoon in late January, and Tess Okafor is reading an email she does not fully understand.

The email is short, and it did not come to her first: Harbor's chief executive sent it on to her an hour ago, adding only four words, *Can you own this?* It comes from a procurement officer at a mid-sized retail chain, a company Harbor Books has been pursuing for four months. Harbor is a thirty-person business-to-business software company in Toronto that makes cloud bookkeeping software for small firms, and this retail chain would be its largest customer by a wide margin. The deal would more or less make Harbor's year, and the sales team has done everything right: the demos went well, and the pricing was agreed last week. Tess, who runs engineering and operations, had assumed the contract was a formality.

The email changes that assumption. After two friendly sentences, it gets to the point: *Before we can move to contract, our security team will need your most recent SOC 2 report. Please send it at your earliest convenience, along with your completed vendor security questionnaire. We can share the questionnaire template if you don't have one.*

Tess reads the email twice. She does not have a SOC 2 report, and she is fairly sure Harbor has never had one, though she is not entirely

certain what one is. She knows it is a security thing, she has noticed the term in the footers of other companies' websites, usually next to a small badge, but she has never had a reason to look closely. Now she has thirty thousand reasons, give or take, and a contract waiting on the other side of a document she cannot produce.

She messages Marcus in sales: *What is a SOC 2 report and do we have one?* Marcus replies in under a minute (*No idea. Thought you'd know.*), which is not encouraging.

Tess does what most people in her position do: she opens a new browser tab and types *what is a soc 2 report* into the search bar. The results are a wall of company blogs, most of them belonging to firms that sell SOC 2 software, each one confident that the answer is to buy their product. Somewhere beneath the marketing is a real answer, and the story this book tells, the whole of it, is what happens between that search and a company that is genuinely ready for an audit, without having panicked, overspent, or bought the first thing a salesperson offered.

The email that started it

Tess's email is the most common way a small company meets SOC 2. Almost nobody goes looking for it; it arrives, attached to a deal, usually from a customer who is bigger than you are.

The pattern is worth slowing down on, because it shapes everything that follows. A small software company spends months building a product and selling it, and it wins smaller customers first: companies its own size, who sign quickly and ask few questions. Then it lands a bigger fish, and the bigger fish has a security team that will not let the company buy software from a vendor it has not vetted. One of the first things that team asks for is a SOC 2 report, and without it there is no contract, so the deal stalls at the finish line.

This is what people mean when they talk about losing a deal over compliance. The product was good enough, the price was right, and the buyer wanted to buy; but the buyer's own rules would not let them sign with a vendor who could not demonstrate, in a way the buyer's

security team trusts, that the vendor handles data carefully. The SOC 2 report is the thing that demonstrates it.

A few hundred kilometres south, in Austin, the same scene is playing out at a much smaller company. Atlas Freight is nine people, and it builds a load-board app, software that helps small trucking carriers find freight to haul. Devin Marsh is the founder and the chief technology officer and, on most days, the entire engineering department. Atlas is pre-seed, which is to say it is running on a tight budget and a lot of hope, and Devin has been courting one large shipper for half a year, a shipper that would be Atlas's first marquee customer, the kind of name that helps raise the next round of funding.

Last week the shipper's procurement team sent Devin the same kind of email Tess received: they want a SOC 2 report before they will sign. Atlas does not have one, nor does it have a security person, a compliance person, or a spare twenty thousand dollars, so Devin has the same questions Tess has, with even less room to get them wrong.

Two companies, very different in size, are both stopped at the same gate, and this is no coincidence. That gate is where this book begins, because it is where most readers are standing when they pick it up.

The feeling, in both cases, is a particular kind of stress. It is not the slow dread of a problem you have been ignoring; it is the sharp jolt of a deadline you did not know existed, attached to money you were counting on. That jolt makes people do expensive, hasty things, sign up for the first tool a salesperson pitches, hire the first consultant who answers the phone, or promise the customer a timeline they cannot meet. The aim of this book is to replace the jolt with a plan, including the answer to the most urgent question of all: what you can honestly tell the procurement team *this week*, which Chapter 3 gives you along with the realistic timeline behind it.

What a SOC 2 report actually is

Here is the one-paragraph version, in plain words.

A SOC 2 report is a document written by an outside accounting firm that examines how your company protects customer data, your security practices, the controls you have in place, and the evidence that those controls actually run, and then writes up what it found. The

report says, in effect, *we examined this company's security controls, and here is our professional opinion of them.* You then share that report with customers who ask for it, so they do not have to take your word for it: an independent third party has looked, and has put its name to what it saw.

That is the heart of it. SOC 2 is a way of demonstrating your security practices to people who have no reason to trust you yet, by having a respected outsider examine them and report on what they find.

A little more detail helps. The letters stand for System and Organization Controls, and the "2" distinguishes it from a couple of related reports the same accounting profession produces. Those reports are governed by standards set by the American Institute of Certified Public Accountants (AICPA), the professional body for accountants in the United States. Only a licensed Certified Public Accountant (CPA) firm can perform a SOC 2 examination and issue the report. That licensing is part of what gives the report its weight, because the firm is staking its professional standing on the opinion it signs.

The examination measures your company against a set of standards called the Trust Services Criteria (TSC), which are the AICPA's published expectations for how an organisation should protect data and run its systems. There are five of them, and most companies, especially small ones, start with just the first, called Security; we will spend a whole chapter on the criteria later. For now, the thing to hold onto is that SOC 2 is not a free-for-all in which the auditor invents their own test. There is a published rulebook, and the auditor checks you against it.

One word deserves a flag here, because the whole framework rests on it: **attestation**. A SOC 2 report is an attestation, which is a specific term in the accounting world: it means an independent professional has examined something and is formally stating an opinion about it, while making clear that the underlying thing, your security programme, remains your responsibility, not theirs. The auditor does not run your security for you; the auditor examines the security you run, and attests to what they find. Keep that word in mind, because it explains a great deal about what SOC 2 is and, just as importantly, what it is not.

There is also a plain-English caveat worth stating early, and it will recur through the book: nothing here is legal advice or audit assurance, but rather general guidance to help you understand the territory and get ready. When the time comes, your auditor forms their own opinion based on your specific facts, and a lawyer advises on your specific contracts. The book informs your judgement; it does not replace the professionals you will eventually work with.

Who asks for it, and why

If almost nobody seeks out SOC 2 on their own, who is doing the asking? Three groups, mostly, and it helps to understand what each of them wants.

Enterprise and mid-market procurement

The first and biggest group is the procurement and security teams at larger companies: your customers, or the customers you are trying to win. This is who emailed Tess and Devin.

When a large company buys software, that software usually touches the large company's data, and sometimes it touches its customers' data too. The buyer is, in effect, handing some of its risk to you, because if you get breached, the buyer's data is exposed and the buyer wears some of the blame. So the buyer's security team has a job: make sure the vendors it lets in are not a soft underbelly. This work has a name, third-party risk management, or sometimes vendor risk management, and it has become a standard part of enterprise buying.

The team running that process cannot personally inspect every vendor's security, since they might be vetting hundreds of vendors a year, so they need a shortcut they can trust. A SOC 2 report is that shortcut: instead of sending their own engineers to examine your systems, they read the report from your auditor and rely on the auditor's independent opinion. One examination, done once a year, answers the same question for every customer who asks, and that efficiency is exactly why the report became standard, because it scales for the buyer in a way that one-off inspections never could.

This is also why the demand has spread so far. A decade ago, a

SOC 2 report was something only larger software companies bothered with, but now it has become a near-default requirement for selling to mid-market and enterprise buyers across North America. Companies routinely lose deals without one, not because the product failed, but because the buyer's own rules forbid the purchase, and the report has quietly shifted from a nice-to-have to a ticket of entry.

Security questionnaires

The second group overlaps with the first, but it is worth pulling out on its own, because it shows up so often. Many buyers do not stop at asking for your SOC 2 report; they also send a security questionnaire: a long list of questions about how you handle data, manage access, respond to incidents, and so on. Tess's email mentioned one, and most do.

These questionnaires can run to dozens or even hundreds of questions, they are tedious to complete, and they tend to arrive with short deadlines. The good news, which we will come back to, is that the work you do to get ready for SOC 2 answers most of the questionnaire too, because the same access controls, the same policies, and the same evidence are the raw material for both. A company that is SOC 2-ready can usually complete a security questionnaire in a fraction of the time it would otherwise take, and with far more confidence, because the answers are backed by genuine practices rather than hopeful guesses.

In fact, having a SOC 2 report often shortens the questionnaire, because a buyer who trusts your report may skip whole sections or accept the report in place of them. That is part of the report's value: it does some of the talking for you.

Answering questionnaires well is a craft of its own, and there is a companion field guide in this same series devoted to it: *Security Questionnaires*, whose TrustReady method we will point you back to when we reach the chapters on vendor reviews. For now, just note that the questionnaire and the SOC 2 report are close cousins, and that getting ready for one largely prepares you for the other.

Investors and the people doing due diligence

The third group is investors, along with the lawyers and analysts who work for them. When a company raises a funding round or gets acquired, the people writing the cheque dig into the business first, and this process, called due diligence, has grown to include security and compliance.

An investor looking at a software company wants to know whether the company can sell to serious customers, so if those customers all demand SOC 2 and the company does not have it, that is a problem hiding in the growth plan. A SOC 2 report, or a credible plan to get one, signals that the company can clear the bar that enterprise buyers set, and it removes a question mark. Increasingly, investors expect to see it, or at least to see that the founders understand it is coming.

Harbor Books is approaching its Series A funding round, and although Tess has not connected the dots yet, the SOC 2 report the retail customer is asking for is the same report Harbor's future investors will ask about. Marlowe Health, a company we will meet shortly, learned this the same way, when the topic came up in both a customer call and an investor call in the same week. The report serves more than one audience at once, because the work you do to win a deal is the same work that reassures the people funding your growth. That overlap is one of the quiet reasons SOC 2 is worth doing properly rather than just barely.

What it is not

A great deal of confusion about SOC 2 comes from misunderstanding what kind of thing it is. So before we go further, it helps to clear away three common misconceptions. SOC 2 is not a certificate, it is not a guarantee, and, for most software companies selling into North America, it is no longer optional.

It is not a certificate

People often say a company is "SOC 2 certified," which is a natural phrase but a wrong one. There is no SOC 2 certificate, and there is no governing body that inspects you, stamps you approved, and adds

you to a registry of certified companies.

What you get instead is the report, that document from the CPA firm, containing their opinion, and it differs from a certification in an important way. A certification is usually pass or fail: you meet the standard and get the badge, or you do not. A SOC 2 report is not pass or fail; it is an opinion, and the auditor can express that opinion in a few different ways.

The opinion comes in four varieties. The one everyone wants is **unqualified**, sometimes called a clean opinion, which means the auditor examined your controls and did not find anything that undermined the picture, your security worked as described. A **qualified** opinion means the auditor found one or more specific problems, which they name in the report, but the rest holds up. An **adverse** opinion means the auditor found problems serious enough that they cannot stand behind the overall picture. A **disclaimer** of opinion means the auditor could not gather enough to form a view at all, often because something went wrong with the examination itself. In practice, almost everyone aims for, and works toward, the unqualified opinion. But the point stands: there is no badge, only a document, and the document carries a graded judgement rather than a simple yes.

This distinction matters more than it might seem. Because the report is an opinion rather than a stamp, the buyer is meant to read it, not merely confirm that it exists, and a thoughtful buyer looks at which criteria you covered, what the auditor tested, whether anything came up, and whether the report is recent. Harbor Books will eventually be on the receiving end of this. Harbor runs its software on infrastructure provided by a larger company called Vantage Cloud, which makes Harbor itself a customer who has to read Vantage's SOC 2 report. When Tess gets there, she will learn to read a report rather than just file it; and she will understand her own report better for having read someone else's.

ISO 27001, which we will meet properly in a later chapter, differs on this exact point, because that one *is* a certification, with a certificate and a certifying body. It is the most common source of the "certified" mix-up, because people assume SOC 2 works the same way. In fact it does not: SOC 2 gives you a report, whereas ISO 27001 gives you a cer-

tificate. Holding the difference in your head now will save confusion later.

It is not a guarantee

A SOC 2 report reduces risk; it does not eliminate it: controls lower the likelihood of problems without removing them entirely.

The second misconception is that a SOC 2 report means a company is secure, full stop: that nothing bad can happen to it. It does not mean that, and no honest auditor would claim it did.

A SOC 2 report describes your security controls and gives an opinion on them, over a defined scope and a defined period: confirmation that sensible practices are in place and running. It does not promise that you will never have an incident. A company with a clean SOC 2 report can still be breached, just as a careful driver can still be hit by someone running a red light; the report says the company is taking reasonable, examined care, not that it is invulnerable.

This is not a weakness of SOC 2 but an honest reflection of how security works, and anyone who promises that a piece of paper makes you safe is selling something. The value of the report is more modest and more real: it gives a buyer good reason to believe you take security seriously and have independent backing for that belief. That is genuinely useful; it is just not a force field.

Keeping this straight protects you in both directions. It stops you from overselling your report to customers, which can come back to bite you if something later goes wrong, and it stops you from expecting too much of it internally: from thinking that once the report is in hand, security is finished. It never is, because the report is a checkpoint on an ongoing road, not a destination.

It is not optional anymore

SOC 2 is now a deal gate, not a differentiator: most mid-market and enterprise buyers in North America require it before signing.

The third misconception is the most consequential, and it is a misreading of the market rather than of the report. Founders sometimes treat SOC 2 as something they can postpone indefinitely, a luxury for

bigger companies, a box they will tick someday, but for a software company selling to mid-market and enterprise customers in North America, that is no longer a safe bet.

The demand has hardened, because as more buyers built vendor risk programmes, asking for SOC 2 stopped being unusual and became routine. Now a small software company that wants to sell upmarket will, sooner or later, encounter a customer who requires it, exactly as Harbor and Atlas did, and at that point the choice is not whether to do SOC 2 but how fast, and whether to do it calmly or in a scramble. Companies do lose real deals over the absence of a report, so the cost of not having one is no longer hypothetical.

This does not mean every company needs SOC 2 on day one, and a two-person startup selling to other tiny startups may not face the question for a while. But any company with ambitions to sell to larger buyers should treat SOC 2 as a *when*, not an *if*, and ideally should begin before the deadline arrives in an email, rather than after, because the companies that handle this well are usually the ones that saw it coming.

There is a parallel pressure outside North America worth naming briefly. In the European Union, a law called the NIS2 Directive is in force across most member states in 2026, and it pushes many companies toward the ISO 27001 standard, so a company selling on both sides of the Atlantic may feel pull from two directions at once: SOC 2 from American buyers, ISO 27001 from European ones. Marlowe Health is in exactly that position, and the good news, again, is that the two frameworks overlap heavily, so the work is not doubled. We will get to that. The point here is simply that for a growing software company, some version of this is coming, and pretending otherwise mostly just shortens the runway when it lands.

What this book covers, and what Volumes 2 and 3 add

This is the first of three volumes, and it helps to know what each one is for, so that you read the right book for where you are.

This book, Volume 1, *Getting Audit-Ready*, has one job: to take you from "a customer asked for our SOC 2" to "we understand what we need, and we are ready for the audit to begin." It is the part most read-

ers need first, because it is the part that turns a confusing email into a clear plan.

Here is the path the book walks. It is laid out in five parts, each building on the one before.

- **Part I: What SOC 2 Actually Is.** The plain-English foundations. What the report is, who performs it, the difference between the two types of report (Type I and Type II), the five Trust Services Criteria, and how SOC 2 relates to ISO 27001 and to the security questionnaires buyers send. By the end of Part I, the vocabulary stops being a fog.
- **Part II: Scoping and Planning.** The decisions that set your cost and effort. What "your system" means and where to draw its boundary, an honest look at what SOC 2 costs and how long it takes, and how to choose between doing it yourself, buying a compliance tool, or hiring help.
- **Part III: The Readiness Assessment.** The heart of the book. How to look honestly at where you stand today, find the gaps between that and what an audit expects, and turn those gaps into a plan you can actually work through. This is where we introduce the book's own framework, the Readiness Ladder, which gives you a simple way to see how far along you are.
- **Part IV: The Controls, in Plain English.** A walk through the actual security practices an auditor will look at (access control, change management, risk and vendor management, monitoring and incident response, and availability and backups) each explained in everyday language, with concrete examples of the evidence an auditor will want to see.
- **Part V: Crossing the Line.** The hand-off. Closing the last gaps, starting the clock on a Type II audit, living the controls day to day, and running the kickoff with your auditor, plus a look ahead to what comes after.

That is Volume 1, and it is deliberately a *readiness* book: it stops at the edge of the audit itself, because getting ready is the part where small teams most often go wrong, overspend, or stall.

Volume 2: The Audit and Operations picks up where this one

leaves off. It covers the auditor relationship and the fieldwork itself, the day-to-day operation of running controls and gathering evidence continuously, what happens at renewal time each year, and a deeper treatment of the ISO 27001 information security management system (ISMS). If Volume 1 gets you to the start line, Volume 2 is about running the race and continuing to run it.

Volume 3: The Operator's Workbook is the hands-on companion: the templates, the policies, the evidence trackers, and the gap-assessment worksheets, the fill-in-the-blanks versions of the tools this book describes. It pairs with a software toolkit for teams who want the worksheets in a more interactive form, so that where Volumes 1 and 2 explain, Volume 3 hands you the instruments.

Each volume stands on its own, so you do not need all three to get value from one, but the set is designed to carry a company the whole way, from the first confused email to a mature, repeatable programme. This book is the beginning of that journey, and for most readers it is the part that matters most, because it is the part that decides whether the rest goes smoothly or painfully.

A word on how to read it. You can go straight through, and the order is built to make sense that way, but you can also use it as a reference once you know the shape, dipping into the cost chapter when you are budgeting, or the access-control chapter when you are fixing that particular gap. The recurring companies are there to help you find yourself in the material, which brings us to them.

Meet the case studies

Throughout this book, the same handful of companies will keep showing up. They are not real names, but they are built from the patterns small software companies actually fall into, and there are four of them, sitting at four points along the path from "just got the email" to "running a mature programme." There is also one recurring person, an outside expert, who advises a couple of them.

The reason for four companies is simple: you are probably reading this because your own company resembles one of these more than the others. When a chapter works through a topic, it will usually lean on whichever company best fits, and tell you what changes if you are big-

ger or smaller. By the end you should be able to point at one of them and say, *that is roughly us*; and, just as usefully, look one rung up the ladder and see where you are heading.

Here they are, smallest and least mature first.

Atlas Freight is the smallest, nine people in Austin, building that load-board app for small trucking carriers. It is pre-seed, with a tight budget and no security staff at all, and Devin Marsh, the founder and chief technology officer, does everything: writes the code, runs the servers, and now, apparently, figures out SOC 2. The trigger for Atlas is the one big shipper who will not sign without a report, and Atlas is our window into the leanest possible version of getting ready, doing it yourself, on a shoestring, with no team and no slack. If your company is tiny and the budget is tighter, Devin is your guide, because much of what Atlas does is about finding the minimum that is genuinely enough, rather than the ideal that is out of reach.

Harbor Books is the company we opened with, around thirty people in Toronto, making cloud bookkeeping software for small firms, and approaching its Series A round. Tess Okafor, the head of engineering and operations, has been handed "the SOC 2 thing" with no playbook and no prior experience, which makes Harbor the book's main protagonist: it is the classic "we got the email, now what" company, and most of the worked examples you will see are Harbor's. It is big enough to need to do this properly, but small enough that there is no dedicated security team to hand it to, which is exactly the squeeze most readers will recognise. One detail to keep in mind, because it comes up more than once: **Harbor Books runs its software on Vantage Cloud's infrastructure**, which makes Harbor a customer of Vantage. So Harbor has to read Vantage's SOC 2 report even as it works to produce its own. It sits on both sides of the relationship, which turns out to be a useful place to learn from.

Marlowe Health is larger and more complicated, around seventy people in Manchester, making patient-intake software for healthcare providers, and expanding into the European Union. Aanya Rao owns security and data protection there. Marlowe faces SOC 2 from its American buyers while, at the same time, contending with ISO 27001 and that NIS2 pressure from its European ones. Because it handles

health information and serves more demanding customers, its scope is wider than Harbor's or Atlas's, it reaches beyond basic Security into the Availability, Confidentiality, and Privacy criteria too. Marlowe is our window into the second framework, the crosswalk between SOC 2 and ISO 27001, and what a broader scope looks like in practice. If you handle sensitive data or sell on both sides of the Atlantic, Aanya's situation will look familiar.

Vantage Cloud is the most mature of the four, around one hundred and eighty people in Denver, a Series B infrastructure software company, with an actual, if small, security team led by Marcus Bauer. Vantage is pursuing both a SOC 2 Type II report and ISO 27001 certification, and it has the headcount and process to run a real programme, so it is our window into what a more grown-up small-company programme looks like, the version Harbor and Atlas may grow into. And, as noted, Vantage is the infrastructure underneath Harbor, which is why Harbor has to read Vantage's report. When we want to show the mature end of the spectrum, or what it means to be the vendor whose report other companies rely on, we will visit Marcus.

Finally, there is **Priya Nair**, who is not a company but a fractional Chief Information Security Officer (CISO), an experienced security leader who works part-time for several small companies at once, rather than full-time for one. She advises Atlas and Harbor, among others, and she is the seasoned outside voice in this book: when a company is about to make an expensive mistake, she is the one who has seen it before. She also stands in for a particular kind of reader, the consultant or managed-service provider who does this work for several small clients and needs to do it efficiently across all of them. So when you see Priya speak, it is usually the voice of someone who has walked this road many times, pointing out where the potholes are.

You will not see all five in every chapter, and that is by design, because the point is not to follow four parallel stories but to give you a cast you can map yourself onto. As the book moves through scoping, costs, the readiness assessment, and the controls, it will reach for whichever company best illustrates the moment, and it will tell you how things shift at a different size. Watch for the company that feels most like yours, and watch for Priya, because her asides are where a

You've just read Chapter 1 of

SOC 2 in Plain English

The full book runs 352 pages across 16 chapters,
with a complete back-of-book index.

Published by Sylvan Press, the book imprint of Sylvan Assurance:
field-tested, plain-English references for the people who do the work.

Scan to see the full book - and where to buy it.
sylvanassurance.com/go/soc2-plain-english

Not ready for the full book? See where you stand first - free, a few minutes:

sylvanassurance.com/go/free-soc2-readiness